Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently amended) A method of supporting multiple encryption schemes over a connection on a network comprising:

transmitting a first request from a source entity to a trusted arbitrator, the first request relating at least in part to establishing a first secure connection between the source entity and a target entity, the target entity being within a local area network (LAN), the LAN coupled to the network and including a connection entity to interact with the trusted arbitrator over the network in setting up the secure connection between the source entity and the target entity;

establishing a second secure connection between the source entity and the trusted arbitrator using a first encryption scheme in response to the first request;

periodically transmitting a second request from the connection entity to the trusted arbitrator to open a third secure connection between the trusted arbitrator and the target entity within the LAN;

transmitting a first response from the trusted arbitrator to the connection entity in response to the second request, the first response informing the connection entity that a request for the first secure connection between the source entity and the target entity exists in the trusted arbitrator~~being associated at least in part with the first request~~; and

establishing ~~a~~the third secure connection between the trusted arbitrator and one of the LAN, the connection entity, or the target entity, using a second encryption scheme in response to the first response, to allow communication between the source entity and the target entity over the first secure connection, the first secure connection comprising the second and third secure connections.

2. (Previously presented) The method according to claim 1, wherein the trusted arbitrator authenticates with the source entity before the second secure connection using the first encryption scheme is established.

3. (Original) The method according to claim 2, wherein the trusted arbitrator supports multiple authentication schemes and determines, before source entity is authenticated, whether a desired authentication scheme used by the source entity is supported.

4. (Previously presented) The method according to claim 1, wherein the connection entity authenticates with the trusted arbitrator before the third secure connection using the second encryption scheme is established.

5. (Original) The method according to claim 1, wherein at least one among the second request and the first response conforms at least substantially to a Hypertext Transfer Protocol.

6. (Original) The method according to claim 1, wherein at least one among the first and second requests is directed to a Uniform Resource Locator associated with the trusted arbitrator.

7. (Original) The method according to claim 1, wherein during at least a part of a period between a time of the transmitting of the first request and a time of the transmitting of the first response, the first request is stored in an area associated with the connection entity in the trusted arbitrator.

8. (Original) The method according to claim 1, wherein if the connection entity does not receive the first response within a predetermined period of a time of the transmitting of the second request, the transmitting of the second request is repeated.

9. (Currently amended) A computer readable medium including computer readable instructions encoded thereon for:

transmitting a first request from a source entity to a trusted arbitrator, the first request relating at least in part to establishing a first secure connection between the source entity and a target entity, the target entity being within a local area network (LAN), the LAN coupled to the network and including a connection entity to interact with the trusted arbitrator over the network in setting up the secure connection between the source entity and the target entity;

establishing a second secure connection between the source entity and the trusted arbitrator using a first encryption scheme in response to the first request;

periodically transmitting a second request from the connection entity to the trusted arbitrator to open a third secure connection between the trusted arbitrator and the target entity within the LAN;

transmitting a first response from the trusted arbitrator to the connection entity in response to the second request, the first response informing the connection entity that a request for the first secure connection between the source entity and the target entity exists in the trusted arbitratorbeing ~~associated at least in part with the first request~~; and

establishing ~~a~~the third secure connection between the trusted arbitrator and one of the LAN, the connection entity, or the target entity, using a second encryption scheme in response to the first response, to allow communication between the source entity and the target entity over the first secure connection, the first secure connection comprising the second and third secure connections.

10. (Previously presented) The computer readable medium of claim 9, further comprising computer readable instructions encoded thereon for authenticating the source entity before the second secure connection using the first encryption scheme is established.

11. (Original) The computer readable medium of claim 10, wherein the trusted arbitrator supports multiple authentication schemes and determines, before the

source entity is authenticated, whether a desired authentication scheme used by the source entity is supported.

12. (Previously presented) The computer readable medium of claim 9, further comprising computer readable instruction encoded thereon for authenticating the trusted arbitrator before transmitting the first response.

13. (Original) The computer readable medium of claim 9, wherein at least one among the second request and the first response conforms at least substantially to a Hypertext Transfer Protocol.

14. (Original) The computer readable medium of claim 9, wherein at least one among the first and second requests is directed to a Uniform Resource Locator associated with the trusted arbitrator.

15. (Original) The computer readable medium of claim 9, wherein during at least a part of a period between a time of the transmitting of the first request and a time of the transmitting of the first response, the first request is stored in an area associated with the connection entity in the trusted arbitrator.

16. (Original) The computer readable medium of claim 9, wherein if the connection entity does not receive the first response within a predetermined period of a time of the transmitting of the second request, the transmitting of the second request is repeated.

17. (Currently amended) A system in a computer network comprising:

a local area network (LAN) including a target entity and a connection entity coupled to the target entity;

~~an access control mechanism coupled to the computer network and to the connection entity of the LAN to control access to the computer network by entities of the LAN;~~

a trusted arbitrator coupled to ~~the access control mechanism~~ the LAN via the computer network; and

a source entity coupled to the trusted arbitrator via the computer network to transmit a first request from to the trusted arbitrator, the first request relating at least in part to establishing a first secure connection between the source entity and the target entity, wherein

the trusted arbitrator establishes a second secure connection between the source entity and the trusted arbitrator using a first encryption scheme in response to the first request;

the connection entity periodically transmits a second request from to the trusted arbitrator to open a third secure connection between the trusted arbitrator and the target entity within the LAN;

the trusted arbitrator transmits a first response to the connection entity in response to the second request, the first response informing the connection entity that a request for the first secure connection between the source entity and the target entity exists in the trusted arbitrator; and

the trusted arbitrator establishes the third secure connection between the trusted arbitrator and one of the LAN, the connection entity, or the target entity, using a second encryption scheme in response to the first response, to allow communication between the source entity and the target entity over the first secure connection, the first secure connection comprising the second and third secure connections.

~~the trusted arbitrator receives a first request for establishing a first secure connection from the source entity to the target entity, the first request relating at least in part to the target entity,~~

~~in response to the first request, a second secure connection is established between the source entity and the trusted arbitrator using a first encryption scheme,~~

~~the connection entity transmits a second request to the trusted arbitrator via the access control mechanism,~~

~~in response to the second request, the trusted arbitrator transmits a first response to the connection entity, the first response being associated at least in part with the first request, and~~

~~in response to the first response, a third secure connection between the trusted arbitrator and the connection entity is established using a second encryption scheme.~~

18. (Cancelled) The system according to claim 17, wherein the third secure connection between the trusted arbitrator and the connection entity is established between the trusted arbitrator and the connection entity using the access control mechanism.

19. (Cancelled)

20. (Original) The system according to claim 17, wherein the trusted arbitrator authenticates with the source entity before the secure connection using the first encryption scheme is established.

21. (Original) The system according to claim 20, wherein the trusted arbitrator authenticates the source entity by verifying identification information sent by the source entity.

22. (Original) The system according to claim 20, wherein the trusted arbitrator supports multiple authentication schemes and determines, before authenticating the source entity, whether a desired authentication scheme used by the source entity is supported.

23. (Previously presented) The system according to claim 17, wherein the connection entity authenticates with the trusted arbitrator before the third secure connection using the second encryption scheme is established.

24. (Previously presented) The system according to claim 23, wherein the trusted arbitrator supports multiple authentication schemes and determines, before being authenticated, whether a desired authentication scheme used by the LAN is supported.

25. (Original) The system according to claim 17, wherein the first request is a query that conforms at least substantially to a Hypertext Transfer Protocol, and the first response is a response that conforms at least substantially to a Hypertext Transfer Protocol.

26. – 29. (Cancelled)

30. (Original) The system according to claim 17, wherein at least one among the first and second requests are directed to a Uniform Resource Locator associated with the trusted arbitrator.

31. (Original) The system according to claim 17, wherein during at least a part of a period between a time of the sending of the first request and a time of the sending of the first response, the trusted arbitrator stores the first request in an area associated with the connection entity.

32. (Original) The system according to claim 17, wherein if the connection entity does not receive the first response within a predetermined period of a time of the sending of the second request, the sending of the second request is repeated.

33. – 37. (Cancelled)